



FortiClient (Linux) - Release Notes

Version 6.2.9

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 26, 2021

FortiClient (Linux) 6.2.9 Release Notes

04-629-740537-20210826

TABLE OF CONTENTS

Change log	4
Introduction	5
Installation information	6
Installing FortiClient (Linux)	6
Installing FortiClient (Linux) using a downloaded installation file	6
Installation folder and running processes	6
Uninstalling FortiClient (Linux)	7
Product integration and support	8
Resolved issues	9
Malware Protection	9
Remote Access	9
Other	9
Known issues	10
Vulnerability Scan	10
Remote Access	10
Other	10

Change log

Date	Change Description
2021-08-26	Initial release.

Introduction

FortiClient (Linux) 6.2.9 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, antivirus, SSL VPN, and Vulnerability Scan features. FortiClient (Linux) can also download and use FortiSandbox signatures.

This document provides a summary of support information and installation instructions for FortiClient (Linux) 6.2.9 build 0418.

- [Installation information on page 6](#)
- [Product integration and support on page 8](#)
- [Resolved issues on page 9](#)
- [Known issues on page 10](#)

Review all sections prior to installing FortiClient.

Installation information

Installing FortiClient (Linux)

You can install FortiClient (Linux) on the following operating systems:

- Ubuntu
- CentOS
- Red Hat

For supported versions, see [Product integration and support on page 8](#).



If upgrading from FortiClient (Linux) 6.0.3 or an earlier version using an RPM package, you must first uninstall any version of FortiClient (Linux) earlier than 6.2.9 from the machine.

If upgrading from FortiClient (Linux) 6.0.4 or a later version, you can directly upgrade to FortiClient (Linux) 6.2.9 without first uninstalling the earlier version of FortiClient (Linux).

Installing FortiClient (Linux) using a downloaded installation file

To install on Red Hat or CentOS:

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:

```
$ sudo yum install <FortiClient installation rpm file> -y
```


<FortiClient installation rpm file> is the full path to the downloaded rpm file.

To install on Ubuntu:

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:

```
$ sudo apt-get install <FortiClient installation deb file>
```


<FortiClient installation deb file> is the full path to the downloaded deb file.

Installation folder and running processes

The FortiClient installation folder is `/opt/forticlient`.

In case there are issues, or to report a bug, FortiClient logs are available in `/var/log/forticlient`.

Uninstalling FortiClient (Linux)

To uninstall FortiClient from Red Hat or CentOS:

```
$ sudo yum remove forticlient
```

To uninstall FortiClient from Ubuntu:

```
$ sudo apt-get remove forticlient
```

Product integration and support

The following table lists version 6.2.9 product integration and support information:

Operating systems	<ul style="list-style-type: none">• Ubuntu 16.04 and later• CentOS 7.4 and later• Red Hat 7.4 and later All supported with KDE or GNOME
FortiClient EMS	<ul style="list-style-type: none">• 6.4.0 and later• 6.2.0 and later
FortiOS	<p>The following FortiOS versions support Telemetry and IPsec and SSL VPN with FortiClient (Linux) 6.2.9:</p> <ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later <p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Linux) 6.2.9:</p> <ul style="list-style-type: none">• 6.4.0 and later
FortiSandbox	<ul style="list-style-type: none">• 3.1.0 and later• 3.0.0 and later• 2.5.0 and later

Resolved issues

The following issues have been fixed in version 6.2.9. For inquiries about a particular bug, contact [Customer Service & Support](#).

Malware Protection

Bug ID	Description
595520	Real-time protection quarantines infected files when action on virus discovery is set to delete infected files.
688229	Antivirus (AV) scan slows down Git cloning.

Remote Access

Bug ID	Description
627855	Third-party multifactor authentication solutions cause SSL VPN authentication to fail.

Other

Bug ID	Description
631550	FortiClient update task fails when attempting to get AV updates from FortiManager.
662719	FortiClient cannot parse configuration when FortiGate pushes 1000 routes.
686443	Command injection.

Known issues

The following issues have been identified in FortiClient (Linux) 6.2.9. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Vulnerability Scan

Bug ID	Description
636209	FortiClient does not accurately or reliably detect Ubuntu.

Remote Access

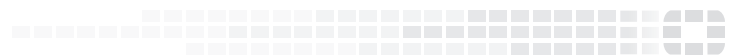
Bug ID	Description
619633	FortiClient cannot connect to SSL VPN without user feedback.
622310	VPN autoconnect when FortiClient (Linux) is offnet.
629821	GUI displays incorrect VPN connection status when VPN is disconnected on the backend.
650340	<i>Unlock Settings</i> button fails to work for FortiClient (Linux) when unregistered.

Other

Bug ID	Description
648101	About page fails to display updated status.
741100	Sandbox test button shows invalid Sandbox IP address for a valid Sandbox.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.